Analyst Insight

Aberdeen Group
A Harte-Hanks Company

January 2012

Left to Their Own Devices: Does Your Enterprise Have a "Dropbox Problem"?

In the absence of *well-defined policies*, *awareness and education*, and *officially supported alternatives* for sharing files securely, knowledgeable end-users will often overlook security and compliance in favor of getting the job done by taking advantage of free and readily available alternatives. Top-performing organizations are able to support the business objectives of end-user productivity, convenience and collaboration while simultaneously sustaining the organization's requirements for security, compliance, and cost-effective management. The key takeaway: don't just keep telling end-users that they're doing something wrong; give them the enterprise-class tools that will help them to achieve their goals, and support them in doing it right.

Business Context: Is it Productive, or Problematic? Yes.

Enterprise data is generally not created to be hidden away – on the contrary, it is generally created to be shared! This truism naturally leads to an increase in the need for enterprise end-users to move it – from person to person, or business to business – as they collaborate with one another. In the absence of well-defined policies, awareness and education, and officially supported alternatives for sharing files securely, however, knowledgeable end-users will often overlook security and compliance in favor of getting the job done by taking advantage of free and readily available alternatives.

Such "rogue" behavior on the part of enterprise end-users taking productivity-oriented information technologies into their own hands – and the challenges this creates for security- and compliance-minded organizations – is anything but new. Ten years ago, it was unauthorized *wireless access points*. Three to five years ago, it was unsanctioned *SharePoint servers* – as Aberdeen wrote about in *Microsoft SharePoint: The Comedy (and Tragedy) of the Commons* (July 2009) – a problem which continues to the present day. Over the last two years, it has been the rapid and remarkable rise of *smart phones* and *tablets* throughout the enterprise, giving rise to the terms *bring your own device* (BYOD) and *consumerization* in the everyday vocabulary of enterprise mobility. As Aberdeen wrote in *Going Mobile* (January 2010), the tide of mobile devices in the enterprise cannot be turned back, and their blended personal / professional use has become the new normal for average end-users, not just the executive ranks.

The "Dropbox Problem" Defined; Déjà Vu All Over Again

In the context of this Analyst Insight, the phrase "Dropbox Problem" is used to represent the generic problem of consumer-oriented file-sharing

Analyst Insight

Aberdeen's Analyst Insights provide the analyst perspective of the research as drawn from an aggregated view of surveys, interviews and analysis.

Fast Facts

Number of mobile apps available in the iTunes App Store under the search phrase "file transfer" as of December 2011

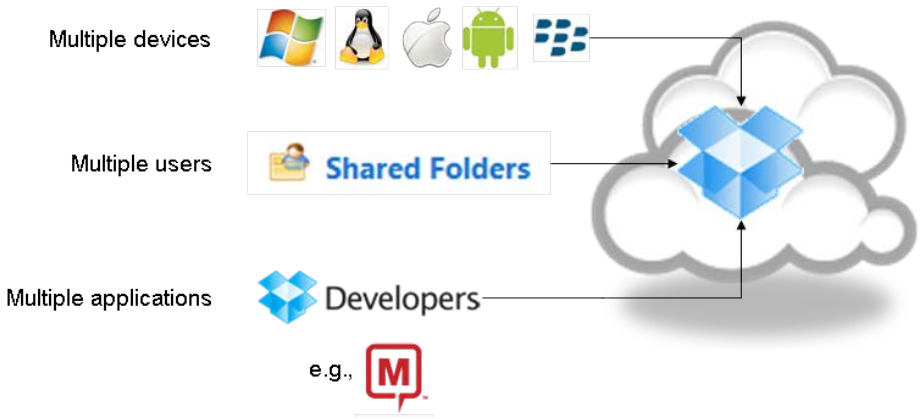
- √ iPhone / iTouch: 131, ranging in price from Free to $37.99
- √ iPad: 74. ranging in price from Free to $9.99

Number of mobile apps available in the Android Market under the search phrase "file transfer" as of December 2011

- √ More than 90, ranging in price from Free to $14.99

solutions which are freely available, extremely easy to use, and generally outside the control of the enterprise IT organization. As a specific example, the *Dropbox* solution is a fantastically useful application that makes it easy for end-users who are mere mortals to access files across *multiple devices* (e.g., their PC at work, their Mac at home, and their iPad, Android smart phone and web browser everywhere in between), share files with *multiple users* (e.g., provide their friends, coworkers, and business partners with direct access to shared folders), and enjoy a common, cloud-based back-end storage infrastructure across multiple applications (e.g., developers such as *Mindjet* can integrate their *MindManager* application such that its files are stored, synched and shared with Dropbox) – see Figure 1. The Dropbox concept is neither new (e.g., the *AOL XDrive* service had launched, and failed, before Dropbox was founded in 2007) nor unique (e.g., consider Microsoft SkyDrive, Apple iCloud and dozens of others), but its popularity is certainly high and growing fast.

Figure 1: Your Sensitive Enterprise Data – Easily Accessible from Multiple Devices, by Multiple Users, by Multiple Applications



Source: Aberdeen Group and www.dropbox.com, January 2012

The obvious problem with the uncontrolled spread of these classes of solutions is that your enterprise end-users are sharing your enterprise data, much of which may be sensitive or subject to security policies or regulatory compliance requirements. Several Aberdeen studies on data loss prevention – see, for example, *Putting the P in DLP* (July 2010) and *DLP, The Ideal Referee: Let the Game Go On* (November 2011) – support the prevailing wisdom that the majority of data loss or data exposure incidents are the result not of the malicious actions of outsiders, but of the inadvertent and well-intentioned actions of insiders. In other words, most incidents are the result of basic human error (inadvertent), and legitimate users who are simply focused on getting their jobs done (intentional, but not malicious).

We Understand the Problem, Now What to Do About IT?

The goal of enterprise security and compliance initiatives is not to "drive incidents to zero" – a goal which might be achieved, for example, by

Fast Facts

Average number of data loss or data exposure incidents experienced in the last 12 months related to file transfer:

√ Best-in-Class: 1

√ Industry Average: 7

√ Laggards: 11

For full details, see *File Transfer is Not What It Used To Be: It's Secure, Reliable, and Well-Managed* (July 2009)

disconnecting everyone from the network, disallowing all access to enterprise applications and data, and saying no to all collaboration and growth opportunities involving file sharing. Clearly these draconian policies would not be in the best interests of most modern businesses.

On the other hand, looking the other way – as end-users attempt to self-manage an array of unsupported devices and unsupported applications, based on unclear or inconsistent policies – exposes the organization to a set of unacceptable (and largely under-recognized) risks to its IT infrastructure and sensitive data. In the absence of well-defined policies, awareness and education, and officially supported alternatives for sharing files securely, end-users will inevitably find their own solutions. As the character Dr. Ian Malcom aptly noted in the movie *Jurassic Park* (1993), "Life finds a way."

Aberdeen's benchmarking style of research shows that the top-performing companies are in fact more liberal than their counterparts in their formal support for mobility and consumer-owned devices, but at the same time they are able to support the objectives of end-user convenience, productivity and collaboration while sustaining the organization's requirements for security, compliance, and cost-effective management. The key takeaway: don't just keep telling the end-users that they're doing something wrong; give them the tools that will help them to achieve their goals, and support them in doing it right.

"Left to their own devices, users were creating their own 'shadow' infrastructure for sharing business information. Rather than invest time and resources in a futile effort to prevent this behavior, it made more sense to give them a solution that can be supported and controlled."

~ Information Security Officer, EMEA-based manufacturer

Aberdeen's Research Findings: Three V's and Three C's

The changing characteristics of the data being used to *enable collaboration between individuals* and to *integrate business processes within and between enterprises* are combining to make secure file sharing solutions more relevant now than ever before. As noted most recently in Aberdeen's report on *Big Data, Big Moves* (July 2011), enterprise data is experiencing exponential expansion along several dimensions, including:

- **Volume** – i.e., the sheer amount of enterprise data that is being created, stored, managed and shared, as well as the sheer size of the files.
- **Variety** – i.e., the proliferation of formats that enterprise data now assumes, particularly in unstructured (file-based) formats such as multimedia (e.g., still images, audio files, video files) and social media.
- **Velocity** – i.e., the speed with which data flows in and out of the enterprise, and the pressure to provide faster access at any time, from any location, from any device.

As the nature of enterprise data is changing, so is the nature of enterprise end-users and the IT infrastructure they use:

- **Collaboration** – The days of enterprise end-users being largely synonymous with internal employees are over. For the average respondent in Aberdeen's *Managing Identities and Access* study (March 2011), for every 100 *employees* there are another 27

Fast Facts

Aberdeen's research on *Real-Time Collaboration* (February 2011) found that the leading performers are 2-times more likely than lagging performers to enforce policies for security and compliance in their solutions for collaboration

Processes to enforce security policies for collaborative tools

√ Best-in-Class: 77%

√ Industry Average: 46%

√ Laggards: 37%

Processes to enforce risk management and compliance standards for collaboration

√ Best-in-Class: 59%

√ Industry Average: 32%

√ Laggards: 23%

temporary employees or *contractors*. Of this combined population, about 2 out of 5 (39%) are supported as *mobile / remote users*. Externally, support for *business partners* and *guests* adds still another 20% to the total end-user count – and this updated figure is then more than doubled when adding in support for the organization's external *customers*.

- **Consumerization** – At the same time, enterprise end-users (of all types) increasingly have an *expectation of access* – increasingly, *wireless* access – to enterprise resources from any place, at any time, from any mobile platform. Of particular note is the growing population of mobile endpoint devices that are *not* managed by the enterprise.
- **Complexity** – This speaks directly to the mounting momentum behind greater diversity and complexity of the enterprise IT infrastructure, and the corresponding challenges to the enterprise's ability to maintain some semblance of visibility and control. In Aberdeen's January 2011 *Network Access* study, for example, about half (49%) of all devices currently supported on the enterprise network were traditional *enterprise-managed* endpoints; more than one-third (36%) were *end-user managed* endpoints, with their fast-changing, consumer-driven lifecycles. The traditional model of one end-user, one device has also broken down – and not just as a perk for senior executives, but for the rank and file employees as well.

Unfortunately, organizations don't have the luxury of dealing with the three Vs and the three Cs in isolation, like the ninjas in an early martial arts movie – these forces are all assaulting the enterprise at the same time. Even as enterprise knowledge workers are becoming more and more independent in terms of their physical location, **secure file sharing** solutions represent one of the core infrastructure capabilities that enable our work lives to be increasingly collaborative and intertwined. Over time, the market has grown and matured from low-level network protocols to full-featured enterprise-class solutions that support secure, reliable and well-managed webs of critical connections. And this in turn is why enterprises should be looking more closely right now at secure file sharing solutions.

Why Traditional Approaches are No Longer Sufficient

As Aberdeen described in *Secure / Managed File Transfer: Why You Should be Looking More Closely Right Now* (August 2011), the most common approaches for sharing files in enterprise scenarios include:

- **Digital "do it yourself"**, which refers to the use of any number of self-service mechanisms to share files digitally, including consumer-oriented "dropbox" solutions, email attachments, non-commercial FTP servers, and in-house programs and scripts.
- **Physical "copy and carry"**, which refers to the use of physical storage media such as tapes, CDs, DVDs, and USB drives to copy digital information and carry it to its intended recipient(s) by

Fast Facts

For the average respondent in Aberdeen's *Managing Identities and Access* study (March 2011):

√ For every 100 *employees*

√ There are another 27 *temporary employees* or *contractors*

√ Of this combined population, about 2 out of 5 (39%) are supported as *mobile / remote users*

√ Externally, support for *business partners* and *guests* adds still another 20% to the total end-user count

√ This updated figure is then more than doubled when adding in support for the organization's external *customers*

courier, overnight delivery services, or other physical delivery mechanisms.

- **Secure file sharing**, which refers to commercially supported file transfer solutions that support multiple file types and protocols; integrate with multiple platforms, applications, and existing IT infrastructure; address security and compliance requirements; and provide reliable, easy-to-use delivery mechanisms and cost-effective management.

Limitations of Digital "Do-It-Yourself" Approaches

In the absence of well-defined policies, awareness and education for end-users, and officially supported alternatives for sharing files, knowledgeable end-users will continue to overlook security and compliance in favor of getting the job done by taking advantage of free and readily available alternatives. Four of the most common are *consumer-oriented "dropbox" solutions*, *non-commercial FTP servers*, transferring files as *email attachments*, and *custom / in-house programs and scripts*.

Limitations with **consumer-oriented "dropbox" solutions** and **custom / in-house programs and scripts** are similar; they include:

- **Unsupported infrastructure** – because these solutions are widely available for free for almost all computing platforms, they have found their way into organizations of every size and can often become embedded in critical workflow. Consumer-oriented solutions likely do not support enterprise-grade requirements. Custom programs and scripts may have been developed by people who have long since left the company.
- **Unenforced policies** – because these capabilities are based on consumer-oriented solutions or custom development at different points in time, they are highly unlikely to reflect the organization's current policies for security and compliance.
- **Unacknowledged risk** – organizations may be dependent on file transfers that continue to take place on a daily basis using these non-supported environments, without making a conscious assessment and acceptance of the inherent risk. The traditional tension between *enterprise policy* and *end-user productivity* plays out most strongly in this area.

Limitations with transferring files as **email attachments** include:

- **File size of attachments** – typical enterprise email configurations restrict attachment sizes to 10Mb or less.
- **Performance** – email was not designed to handle extremely large files, and their timely and reliable delivery often proves problematic.
- **Storage** – large attachments (often multiple copies of large attachments) quickly eat up allocated storage; small attachments

with widespread distribution (e.g., 3Mb x 1,000 employees) can have the same effect.

- **Security and compliance** – too often, policy is left to proper actions being taken by individual end-users, versus being automated by solution providers.

Limitations common with **non-commercial FTP servers** include:

- **No inherent method for encryption** – data is sent in the clear; extensions such as SFTP or FTPS can be confusing and difficult to use in an interoperable manner.
- **Require action to be taken by a system administrator** – requests to enable a new FTP account can take hours or days to be fulfilled, and time-sensitive file transfers can suffer unacceptable delays.
- **Manual processes** – e.g., files placed on an FTP server stay there until manually deleted.
- **Insecure servers** – end-users may often have access to data on FTP servers that is not intended for them.
- **Lack of many other useful mechanisms** – e.g., FTP servers lack sender verification that a transfer is complete, and receiver verification of the integrity of the file received.

Fast Facts

The *File Transfer Protocol (FTP)* refers to the venerable industry standard network protocol used to exchange and manipulate files over IP-based computer networks. FTP dates back to April 1971, when the IETF Network Working Group first described the protocol that had been developed "for immediate implementation on two hosts at MIT" (see RFC 114). Because the original FTP specification did not describe a method for transferring files securely, extensions were developed over the years to leverage the cryptographic security capabilities of later network protocols such as *Secure Shell (SSH)*, *Secure Sockets Layer (SSL)* and *Transport Layer Security (TLS)*.

Limitations of Physical "Copy and Carry" Approaches

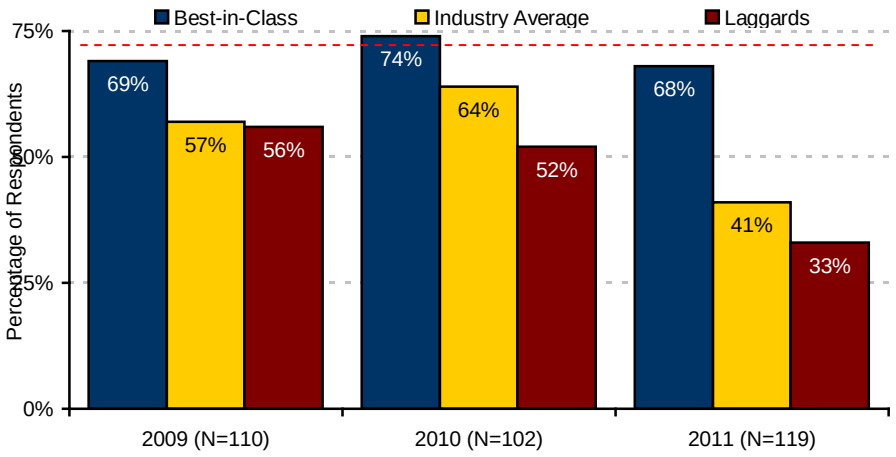
The process of creating, dropping off and delivering physical media for expedited shipment can be error-prone, time-consuming and costly. And even with same-day or overnight delivery services, direct file transfer is always faster – with reduced carbon emissions from the fuel used for physical transportation as an added, environmentally-friendly benefit.

Another consideration is the security of data transported in portable physical containers such as tapes, removable media (e.g., CD, DVD), and USB drives. Even when the media arrives at the intended recipient, for example, do you know who may have accessed or copied your critical data? Many companies use *encryption* to provide *data confidentiality* and *data integrity*, but this can add considerable cost, complexity and time to an approach which is supposed to be simple. In the current business climate, securely and reliably sending the bits while simultaneously reducing costs can make an extremely compelling value proposition.

Market Trends: Selected Aberdeen Research Findings

In the course of conducting its benchmark style of research, Aberdeen routinely asks about the *current use*, *planned use* in the next 12 months, and *current evaluations* of enabling technologies such as secure file sharing. In comparing findings of this nature from three independent studies conducted in 2009, 2010 and 2011, there is a general trend across all respondents towards greater use of secure file sharing – this is consistent with both the business context and the limitations of common alternatives, as discussed above. Moreover, the use of secure file sharing is consistently correlated with the companies achieving top performance (see Figure 2).

Figure 2: Current Use of Secure File Sharing Consistently Correlates with the Companies Achieving Top Performance



Source: Aberdeen Group, July 2011

In another view of these findings (Figure 3), the current use of secure file sharing is seen to be an increasingly strong *differentiator* of top performance. That is, the percentage of adoption by the leading performers is consistently high, but the *ratio* of adoption by the leading performers compared to that of the lagging performers is seen to increase over time.

In other words, the evidence is that the top performers continue to address the need to share data through secure, reliable and well-managed commercial solutions – while all others, perhaps overwhelmed to some degree by the three Vs and three Cs discussed earlier, may be losing control of their policies and processes in this area. Once again, this is why enterprises should be looking more closely right now at secure file sharing solutions.

Figure 3: Current Use of Secure File Sharing is Increasingly a Differentiator of the Companies with Top Performance

Source: Aberdeen Group, July 2011

Finally, a closer look at the most recent findings – from the *Q1 2011 Aberdeen Business Review* (May 2011) – show that there is little difference in current use by geographic region or by industry segment. Current use is higher among Large (>$1B in annual revenue) enterprises, however, consistent with their generally greater complexity and scale (Table 1).

Definitions

For this Analyst Insight:

- √ **Baseline** refers to high adoption by the leading performers, as well as relatively high adoption by all others.
- √ **Emerging** refers to modest adoption by the leading performers, and relatively low adoption by all others.
- √ **Early Adoption** refers to modest adoption by the leading performers, but high adoption by the leaders relative to that of all others.
- √ **Differentiators** refers to high adoption by the leading performers, and high adoption by the leaders relative to that of all others.

Definitions

- √ **Large:** revenue of $1B or higher in the last 12-month reporting period
- √ **Mid-Size:** less than $1B and more than $50M
- √ **Small:** $50M or lower

Table 1: Secure File Sharing – Analysis by Geography, Industry Segment, Company Size

	Geographic Region of HQ			Industry Segment			Company Size by Revenue		
	Americas	EMEA	A / P	Tech	Services	Manufact.	Small	Mid-Size	Large
Current	71%	72%	69%	67%	69%	70%	64%	66%	**83%**
Plan / Eval	21%	21%	27%	24%	22%	15%	27%	24%	15%
No Plans	8%	7%	4%	9%	9%	15%	9%	10%	2%

(N=151) Source: Aberdeen Group, July 2011

Characteristics of Enterprise-Class Secure File Sharing

As a prime example of the modern "plumbing" that supports collaboration and integrates business processes, secure file sharing solutions have specifically been designed to liberate the enterprise from the cost and

complexity of managing file transfers in the typical heterogeneous IT computing infrastructure, and to address the many shortcomings of the physical "copy and carry" and digital "do-it-yourself" approaches. Key capabilities of these solutions are likely to include the following:

- **Support for Multiple Enterprise Platforms** – e.g., Windows, Mac OS X, Linux, Solaris, HP-UX, AIX, AS/400, System z
- **Support for Multiple Mobile Devices** – e.g., Apple iOS, Google Android, RIM Blackberry, Windows Phone 7
- **Support for Multiple File Types** – e.g., Adobe PDF; Microsoft Office documents, presentations, spreadsheets; email; Web pages (HTML, XML); multi-media files (still images; audio; video); EDI (X12, EDIFACT, ASNI X.12); custom / in-house formats
- **Integration with Applications and IT Infrastructure** – e.g., Web browsers, email clients, graphics applications, identity and access management repositories (Microsoft Active Directory, LDAP, RDBMS)
- **Secure and Reliable Delivery Mechanisms** – e.g., support for guaranteed file delivery; automatic retry and restart from the point of transmission failures; authenticated file receipt
- **Cost-Effective Management** – e.g., centralized control over policies; automation of scheduling and workflow; system-wide visibility of file transfer activities for auditing and reporting

These capabilities are not intended to be comprehensive, but to illustrate the surprising complexity that can be involved in the simple notion of transferring a file from point A to point B! All the more reason to look more closely at enterprise-class secure file sharing solutions, rather than muddle along with risky and outdated digital do-it-yourself or physical copy-and-carry approaches.

A growing number of organizations are attracted to the benefits of cloud-based delivery models for secure file sharing, as opposed to traditional on-premise solutions. In Aberdeen's *Q1 2011 Aberdeen Business Review*, about 1 in 5 (19%) of all respondents – and one-third (33%) of Small businesses (less than $50M in annual revenue) – indicated current use of a Software-as-a-Service (SaaS) model.

Common Use Cases for Secure File Sharing

Another important aspect of aligning the organization's current and future needs for secure, reliable file transfer with the capabilities of prospective secure file sharing solution providers are the intended *use cases*. The vast majority of use cases supported by consumer-oriented secure file sharing solutions would be categorized as **person to person** (i.e., an individual sender sharing files with one or more specific receivers) and **ad hoc** or **on demand** (i.e., file sharing that is initiated as needed, as opposed to at a specific scheduled time) – reflecting the essential nature of *collaboration*.

Solution Selection Criteria

Factors to consider when evaluating secure file sharing solutions:

√ Ease of use

√ Security and compliance capabilities

√ Integration with multiple enterprise platforms, mobile devices, applications, and existing IT infrastructure

√ Support for multiple file types and protocols

√ Secure and reliable delivery mechanisms; cost-effective management

√ Ability to scale

√ Total cost of ownership

√ Vendor reputation, customer base, and support

Fast Facts

Current use of a cloud-based (e.g., SaaS) deployment model for secure file sharing:

√ All respondents: 19%

√ Small businesses: 33%

Customer Case in Point: Engineering Firm, Canada

Founded in 1956, Toronto-based Halsall Associates provides personalized engineering services – including building design, building evaluation and renewal, and green strategies for facilities and communities – to clients around the globe. Timely information exchanges drive Halsall's operations, with the firm's 340 employees collaborating with colleagues and clients on a daily basis, using very large data files such as computer-aided design (CAD) files, floor plans and contract documents.

Traditionally, employees relied on the IT department to create an FTP site, or they copied files to a CD or thumb drive – both inefficient and time consuming options. Transferring very large files by email just wasn't possible. More critically, existing methods were simply delivery mechanisms, and none provided the true document sharing capabilities that Halsall really needed.

"Creating a self-service collaborative environment was key for us – allowing employees to work smarter, faster, and more effectively," said Noman Ahmed, IT Infrastructure Specialist with Halsall Associates. "We wanted to allow employees and clients to share information when and where needed without relying on IT – focusing on the project at hand and improving the level of customized service."

After investigating several solutions, Halsall selected Accellion Secure Collaboration based on its capabilities for file collaboration, ease-of-use, and end-user file management. Employees simply need a client's email address to create a new workspace, and are then are free to upload and download files as often as needed, with authorized users notified when new or updated documents are available. From the initial tender process, to collaborative design and engineering, to ongoing project management and support, the Accellion solution supports the entire project lifecycle while putting the power of business communications into the hands of employees and clients.

The IT department retains full visibility, with an automated audit trail of file access activity by sender, recipient, file size, date sent, and date accessed. In addition, integration with Active Directory eliminated the need for end-users to remember additional passwords and for IT to create and delete accounts due to personnel changes.

"We are enhancing our collaborative work environment," said Ahmed, "And responding to the needs of our clients faster than ever before."

"Everything we do is based on a collaborative, team-based approach, so we needed a solution that supported this philosophy. Now, our staff does not think twice about how to share documents. The Accellion solution is the go-to source for all internal and external interactions."

~ Noman Ahmed,
IT Infrastructure Specialist,
Halsall Associates

Solutions Landscape (illustrative)

Solution providers for secure file sharing have evolved from a wide variety of corporate heritages; Table 2 provides a partial list.

Table 2: Solutions Landscape for Secure File Sharing Solutions (illustrative)

Company	Web Site	Solution(s)
Accellion	www.accellion.com	Accellion Secure Collaboration, Accellion Secure File Transfer, Accellion-in-the-Cloud, Accellion Mobile Apps for iPad and iPhone
Axway	www.axway.com	Axway SecureTransport, File Transfer Direct
Box	www.box.com	Box Business and Enterprise, Box Mobile API
Biscom	www.biscomdeliveryserver.com	Biscom Delivery Server (BDS)
GlobalSCAPE	www.globalscape.com	Enhanced File Transfer (EFT) Server, Managed Information Xchange (MIX) service
Ipswitch	www.ipswitch.com	MOVEit, MessageWay
Oxygen	www.oxygencloud.com	Oxygen Pro Cloud, Oxygen Enterprise Cloud
SugarSync	www.sugarsync.com	SugarSync, SugarSync Mobile App
TIBCO Software (Proginet)	www.tibco.com www.proginet.com	TIBCO Managed File Transfer, TIBCO Slingshot
YouSendIt	www.yousendit.com	YouSendIt Enterprise Management Services (EMS), YouSendIt Mobile App

Source: Aberdeen Group, January 2012

Summary and Recommendations

Regardless of the specific technology used in support of collaboration and sharing of enterprise data, Aberdeen's research has consistently shown that the following general steps are consistent with top performance:

- **Assign clear ownership and accountability** for data protection initiatives to an executive or cross-functional team. The "one throat to choke" principle is consistently correlated with the achievement of top results.
- **Identify and classify your data.** You can't protect what you don't manage, and you can't manage what you don't know about.
- **Inventory existing file sharing activities** to establish a baseline for use cases, volumes, frequency, methods, applications and end-users. You can't manage what you can't see, and the research indicates that for most companies much of the file transfer activity takes place below the surface.
- **Consider secure file sharing for mobile devices** explicitly, to head off the "Dropbox Problem" and support enterprise end-users

with the tools they need, rather than leaving them (literally) to their own devices.

- **Prioritize your security control objectives** for information assets – and particularly file transfer data – as a function of risk, audit, and compliance requirements. Not all data is worth being protected; you should prioritize the protection of the data with the greatest impact on the business.
- **Establish consistent policies for file sharing**, including inbound, outbound, and internal to the organization, as part of an overall approach to safeguarding sensitive data. Data is flowing everywhere, all the time.
- **Invest in documentation, awareness, and training** for end-users, who should be made fully aware of their responsibilities for protecting the organization's sensitive data. Investments in technologies to help protect data can be significantly eroded by insufficient investments in the people and process side of successful implementation.
- **Select and deploy a secure file sharing solution**, and deliberately move away from the tangled, digital do-it-yourself approaches to file transfer taken in the past in favor of implementing a common enterprise secure file sharing solution or "platform." The choice of an on-premise or SaaS-based solution should be based not only on an analysis of cost, but also on an analysis of acceptable levels of risk. Secure file sharing solutions should integrate with key applications, and when appropriate should integrate with existing identity and access management infrastructure and data loss prevention infrastructure as well.
- **Measure and monitor** all file transfer activity; regularly review and analyze data from management and reporting systems; drive continuous improvements by finding and eliminating root causes for exceptions, security events, and audit deficiencies.
- **Automate enforcement** of file transfer policies whenever reasonable, with notification to end-users; standardize audit, analysis, and reporting. Both will reinforce awareness of policies and expectations for ongoing behavior.

Every organization is somewhere along this path, and for the business-oriented purchaser / decision maker this list should be helpful in *asking the right questions*, both internally and externally (e.g., of product and services providers), about proposed solutions and implementation plans.

Explicit acknowledgement of the need to support **collaboration** as a driver for current investments in protecting and managing unstructured data underscores the slow but steady shift in the perception of enterprise IT Security from one of being an *obstacle*, to one of being an *enabler*.

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research	
DLP, The Ideal Referee: Let the Game Go On; November 2011	*Going Mobile*; January 2010
Secure / Managed File Transfer: Why You Should be Looking More Closely Right Now; August 2011	*File Transfer is Not What It Used To Be: It's Secure, Reliable, and Well-Managed*; July 2009
Big Data, Big Moves; July 2011	*Microsoft SharePoint: The Comedy (and Tragedy) of the Commons*; July 2009
Q1 2011 Aberdeen Business Review; May 2011	*Securing Unstructured Data: How Best-in-Class Companies Manage to Serve and Protect*; June 2009
Real Time Collaboration: Innovate Your Business and Increase Revenue; February 2011	*Safe Email: Seven Important Tips for Better Email Security*; June 2009
The CIO's View of Data Protection: Seven Symptoms to Self-Diagnose Your Data Protection Initiative; August 2010	*Managing Encryption: The Keys to Your Success*; October 2008
Putting the P in DLP; July 2010	*Secure / Managed File Transfer*; September 2008
Content Aware: The 2010 Data Loss Prevention Report; June 2010	

Author: Derek E. Brink, Vice President and Research Fellow, IT Security (Derek.Brink@aberdeen.com)